REMARKS

Claims 105-128 were pending in the application. Claims 105, 107, 115-118, and 127-128 have been amended. Claims 108, and 119-126 have been cancelled. Claims 129-149 have been added. Accordingly, claims 105-107, 109-118, and 127-149 remain pending in the application.

Applicant is in receipt of the Office Action dated March 8, 2007.

REJECTIONS UNDER 35 U.S.C. §103

The Examiner has rejected the claims under 35 U.S.C. §103(a) as being obvious over Balasubramaniam et al., U.S. Patent No. 6,671,812 in view of Muttik, I., U.S. Patent No. 6,770,780. Applicant disagrees with these rejections, and submits that the previous versions of the claims patentably distinguish over the cited art. Nonetheless, in order to expedite prosecution, Applicant has amended the pending claims, which are believed to be in condition for allowance.

Balasubramaniam is directed to "cleaning a computer" involving "delet[ing]" "undesired data and software." Balasubraminiam, Abstract. The problem addressed by Balasubramaniam is "a need for an automatic method and system to clean up a computer storage." Id., at col. 2, lines 2-3, emphasis added. The method of Balasubramaniam involves "a search of the user computer's storage medium, for example, in the cache area of the browser." Id. at col. 10, lines 26-28 (emphasis added). In other words, the reference teaches using "a software program called QuickClean.TM., designed to 'cleanup' the user's **hard drive**." *Id.* at col. 6, lines 44-46 (emphasis added).

The Examiner has cited Balasubramanian as disclosing "selecting an active program on a computer system as code under investigation, wherein at least some of the code associated with the selected active program is running in kernel mode," as recited in claim 105. Applicant respectfully disagrees. As stated above, Balasubramaniam is directed to a method to "cleanup" a "user's hard drive." Accordingly, there appears to be no teaching or suggestion in the reference of "selecting an active program," as recited in claim 105 (emphasis added). Accordingly, there is no disclosure that "the

selected active program is running in kernel mode," as also recited in claim 105. Applicant thus disagrees with the Examiner's characterization of the Balasubramaniam reference.

Muttik also does not teach or suggest claim 105's recitation of "wherein at least some of the code associated with the selected active program is running in kernel mode" (emphasis added). In contrast, Muttik teaches that:

> Emulator 110 includes emulator buffer 201, emulator code 203, comparison unit 204, database 206 and rules 210. Emulator buffer 201 is a protected region of memory (also known as a sandbox) in which code 108 is stored and emulated. Emulator code 203 includes code to perform the emulation. Emulator buffer 201 and emulator code 203 are designed so that code 108 that is executing within emulator buffer 201 **cannot damage or compromise** computer system 106.

See Muttik, col. 3, lines 54-65 (emphasis added). Applicant respectfully submits that, in Muttik, since "code 108 that is executing within emulator buffer 201 cannot damage or compromise computer system 106," it cannot include "code" that "is running in kernel mode," as is recited in claim 105. *Id.* Furthermore, Applicant submits that it would not be obvious to modify Muttik such that "at least some of the code associated with the active program program is running in kernel mode" since doing so would render Muttik inoperable for its intended purpose, preventing "damage or compromise" to "computer system 106." Similarly, neither Balasubramaniam nor Muttik teaches claim 115's "wherein said code is running in a manner that permits infection of said computer system." Claim 115 and its dependent claims are believed patentably distinct over the cited art for at least this reason. Claims 127 and 128 are also believed to be patentably distinct for reasons similar to those provided for claim 105.

***

Applicant also submits that the cited references, whether taken singly or in combination, do not teach or suggest the features of "a first and second plurality of detection routines" recited in claim 105. Specifically, Applicant submits that the cited art does not teach or suggest, among other things, "weighting each of the first plurality of results to obtain a first score indicative of whether the code under investigation is valid code" and "weighting each of the second plurality of results to obtain a second score indicative of whether the code under investigation is malicious

code." Muttik, in contrast, merely teaches that "comparison unit 204 can be configured to assign weights to system calls. Weights can be positive for suspicious activity, and negative for activity...present in non-malicious code," Muttik, col. 5, lines 14-17, and then refers to "a count of the **total weight**, which is compared against a threshold value." *Id.*, col. 5, lines 18-19 (emphasis added). At a minimum, then, Muttik does not teach the "first score" and "second score" of claim 105. Balasubramaniam is believed to have no teachings pertinent to these features of claims 105.

Accordingly, claim 105 and its dependent claims are believed to patentably distinguish over the cited art for these additional reasons. These additional reasons apply equally to independent claims 115, 127 and 128 (and, by extension, to their dependent claims).

Thus, claims 105, 115, 127 and 128, along with their respective dependent claims, are believed allowable.

CONCLUSION:

Applicants submit the application is in condition for allowance, and an early notice to that effect is requested.

The Commissioner is authorized to charge any fees that may be required, or credit any overpayment, to Meyertons, Hood, Kivlin, Kowert & Goetzel, P.C. Deposit Account No. 501505/6002-00602/DMM.

Respectfully submitted,

Date: May 8, 2007

By: /Dean M. Munyon/
Dean M. Munyon
Reg. No. 42,914

Meyertons, Hood, Kivlin, Kowert & Goetzel, P.C.
P. O. Box 398
Austin, Texas 78767
(512) 853-8847